invention, is incorporated herein by reference. See also Sandhu et al, "Proceedings of the First ACM Workshop on Role Based Access Control", ACM, 1996, also not prior art to the present invention.

Despite the existence of extensive literature on the subjects of both RBAC and MLS sytems, insofar as known to the inventor the prior art does not suggest application of RBAC to MLS systems without disturbance of the underlying MLS "kernel", which is essential if MLS's advantages, and the investment therein, are to be preserved.

Finally, also of general interest to the present invention is European Patent Application 94 112 649.2 (IBM), showing a hybrid RBAC system, wherein role assignments are apparently used to generate access control lists corresponding to objects. This application does not refer to MLS systems.

OBJECTS OF THE INVENTION

It is therefore an object of the invention to provide a method whereby access of individuals and subjects to objects controlled by an MLS system can be simplified using RBAC as an interface to the MLS system.

It is a further object of the invention to provide a method for employment of RBAC as an access method for MLS systems, without disturbance of the MLS kernel, thereby preserving the security advantages provided by MLS.

It is a further object of the invention to provide a method for employment of RBAC as an access method for MLS systems while simultaneously preserving the traditional methods of access to MLS, whereby objects protected by the MLS system can be accessed through RBAC or by traditional methods.

SUMMARY OF THE INVENTION

According to the invention, each role within an RBAC system is treated as a collection of permissions on privileges, that is, the right to access a set of objects. RBAC is implemented on an MLS system by establishing a mapping between privileges within the RBAC system and pairs of levels and sets of "compartments" assigned to objects within the MLS system. The advantages provided by RBAC, that is, reducing the overall number of connections that must be maintained, providing access to protected objects in a manner conveniently mirroring the organizational structure, and greatly simplifying the process required in response to a change of job status of individuals within an organization, are then realized without loss of the security provided by MLS.

To implement RBAC in an MLS environment, a trusted interface function is developed to ensure that the assignment of levels and sets of compartments to users is controlled according to the RBAC rules; that is, the trusted interface ensures that the RBAC rules permitting individuals membership in roles are followed rigorously, and provides a proper mapping of the roles to corresponding pairs of levels and sets of compartments. No other modifications are necessary. Access requests from subjects are first mapped by the interface function to the pairs of levels and sets of compartments available to the corresponding role, after which access to the objects is controlled entirely by the rules of the MLS system, responsive to the pairs of levels and sets of compartments assigned.

In essence, each user request for a privilege is checked to ensure that it is permitted to the subject's role at the time of the request. The trusted interface then sets the subject's compartments and levels according to a mapping function that determines a unique combination of compartments and levels for the privilege requested.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be better understood if reference is made to the accompanying drawings, wherein:

FIG. **1**, as discussed above, shows schematically the assignment of objects protected by a MLS system to compartments and levels, thus forming a lattice;

FIG. **2** shows schematically the relation between subjects, roles, and operations according to the RBAC model;

FIG. **3** shows schematically the arrangement of RBAC as the access method employed with an MLS system;

FIG. **4** shows a diagram similar to that of FIG. **1**, and additionally illustrates the manner in which objects protected by an MLS system can be accessed through the RBAC interface, accessed as previously provided, or both;

FIG. **5** shows an example of compartment labeling for a heirarchical privilege set; and

FIG. **6** shows an enlarged portion of FIG. **2**, with privilege sets associated with various roles.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Role based access control (RBAC) is offered as an alternative to traditional discretionary (DAC) and mandatory access control (MAC) systems for controlling access to computer systems; that is, RBAC is normally considered an alternative to access control list and "multi-level secure" ("MLS") systems, respectively. See the prior art Ferraiolo et al 1992 and non-prior art Sandhu 1996 papers discussed above. RBAC is attracting increasing attention, particularly for commercial applications.

The principal motivation behind RBAC is the desire to specify and enforce enterprise-specific security policies in a way that maps naturally to an organization's structure. Traditionally, managing security has required mapping an organization's security policy to a relatively low-level set of controls, typically access control lists.

With RBAC, security is managed at a level that corresponds closely to the organization's structure. Each user is assigned one or more "roles", and each "role" is assigned one or more "privileges" that are permitted to users in that role.

FIG. **2** shows schematically the organization of a conventional RBAC system. Subjects **20**, which can include external programs **22**, external systems **24**, or individual users **26**, who will normally be identified to the system through a conventional identification process **28**, are assigned to roles **30**. The subjects **20** can then perform operations **32** as assigned to the roles **30**.

In this connections, "operations" includes "privileges", including the right to access objects within the protected system, such as stored documents, or to employ resources, or to perform certain "transactions". The operations provided for each role correspond to the duties and responsibilities of the persons having that role in the organization. For example, roles in a bank may include the role of teller or accountant. Each of these roles has a set of privileges or transactions that they can perform, including some privileges that are available to both roles. Roles can be hierarchical. For example, some roles in a hospital may be health care provider, nurse, and doctor. The doctor role may include all privileges available to the nurse role, which in turn includes all the privileges available to the health care provider role.